Non-Repudiation-based Network Security System using Multiparty Computation

Divya K.S[1]
Research Scholar, GSSS Institute of Engineering and Technology for Women, Mysuru, India

Roopashree H.R[2]
Associate Professor, GSSS Institute of Engineering and Technology for Women, Mysuru, India

Yogeesh A C[3]
Assistance Professor
Government Engineering College
Kushalnagar, India

Abstract*—Security has always been a prominent concern over the network, and various essential requirements are required to cater to an efficient security system. Non-repudiation is a requirement about the non-deniability of services acting as a bridge between seamless relaying of service/data and efficient security implementation. There have been various studies carried out towards strengthening the non-repudiation system. There are certain pitfalls that render inapplicability on dynamic cases of vulnerability. The conventional two-party non-repudiation schemes have been widely explored in the existing literature. But this paper also advocates the adoption of multi-party computation, which has better feasibility toward strengthening a distributed security system. The current work presents a survey on the existing approaches of non-repudiation to investigate its effectiveness in the multi-party system. The prime aim of the proposed work is to analyze the current research progress and draw a research gap as the prominent contribution of the proposed study. The manuscript begins by highlighting the issues concerning multi-party strategies and cryptographic approaches, and the security requirements and standardization are briefly discussed. It then describes the essentials of non-repudiation and examines state-of-the-art mechanisms. Finally, the study summarizes and discusses research gaps identified through the review analysis.

Keywords*—*Future network; multiparty computation; nonrepudiation; security

I. Introduction

The computational infrastructure has evolved from desktop computing to distributed architecture of computing. To elaborate further, it can be said that the ecosystem of the computation has evolved periodically from desktop computation to the client-server, and after the event of the internet, the model of the web-server-based applications. The new dimension of a highly scalable infrastructure includes cloud computing and the Internet of Things (IoT) [1][2]. The various applications are running on these distributed architectures, which are critical for different walks of life, including defense, government, e-commerce, e-hospitals, education, etc., in the form of context-oriented pervasive and ubiquitous manner. In any computing model, reliability becomes a primary requirement once it matures because the system has various vulnerabilities, and those vulnerabilities pose multiple threats to the system [3]. A direct attack on the system introduces the failure of the entire system; therefore, appropriate security measures must be researched and developed according to the changing dynamics of the computing environment. The reliable security system must comply with the essential consideration of practical aspects for Confidentiality, Integrity, Authentication, Availability, Authorization, Access Control, and Non-repudiation [4][5]. The robust security in such distributed architecture means that multiple parties or entities must collaborate to generate security attributes. One such popular technique is "Multiparty Computation," which collects the inputs from various participating entities to preserve or isolate their privacy from the other parties [6]. A function generates the output based on these inputs. The focus of the current paper is to study the research trend on the non-repudiation aspects. The common word meaning of repudiation is to deny. In digital security systems, the transaction occurs between the stakeholder or the different parties for the authentication or the security protocol requirements. Therefore, both parties cannot deny that the sender does not send either message and is not received by the receiver. The guarantee of non-denial is the authentication of the signature or message or the document or, in general, any attributes defined as non-repudiation. Various network architectures, including wireless vehicle network, Wireless Sensor Networks (WSN), Internet of Things (IoT), etc., demand customized security solutions. The popular techniques used in the security domain include Public Key Cryptography (PKC), Digital Signature (D.S.), digital certificate (D.C.), hashing, and critical public infrastructure (PKI). Symmetric Key Cryptography (SKC), etc. [7]-[10]. There is a challenge that the method adopted should be suitable for most of the essential requirements of the security protocols, or at least the process for non-repudiation should also complement another security requirement. This paper critically analyses the various approaches used for the non-repudiation protocol design in general and specific to the different networks. Further, this paper focuses on the research approaches adopted for designing a non-repudiation scheme using multi-party computation. The proposed manuscript offers updated information about multi-party security solutions towards non-repudiation. Therefore, it is essential to gather research trends in this direction and make the information available to the researchers interested in security protocol design, especially for non-repudiation using multi-party computation. The contribution of this paper is as follows: The initial Section II of the paper provides conclusive information from the journal of Onieva et al. [11], and then in Section III, the methodology for the literature data collection is described. Section IV discusses the approaches toward non-repudiation, while Section V discusses multi-party non-repudiation schemes. In contrast, Section VI discusses open research issues, and Section VII discusses the contribution of this paper.

II. Essentials of Non-Repudiation

This section highlights the significance of non-repudiation and multi-party non-repudiation with respect to design perspective.

A. Design Parameters for Non-Repudiation Protocol

Whenever the transactions occur between two parties, there is a fair chance of disputes due to complete or conditional denial of the transaction. The security service which tries to resolve by a fair settlement is called Non-Repudiation (N.R.). Generally, this problem is also to analyze the behavior of the involved activities, and the first standardization was defined in 1996 by ITU as ITU-X.813 [11]. Fig. 1 illustrates a correlation between the different phases of the N.R. service. The typical stages of the non-repudiation process, such as evidence generation, evidence transfer, storage and retrieval, and evidence verification, includes the transaction (T)= {E, I, O, R, R.V.}, where E=evidence, I=information, O= observation, R= request generation and RV= request verification. In the last phase, dispute resolution, the defendant and the plaintiff process their justification with the agreed adjudicator in the non-repudiation service. The message communication occurs either directly or through a delivery agent from the source node to the destination node. For the accountability of the sender and receiver node, services like non-repudiation of origin and non-repudiation of receipt are essential. If the dispute occurs where the delivery takes place through the delivery agent, the NR-services require N.R. of submission and N.R. of delivery. The evidence stored either digitally signed using PKC or as secure envelopes using SKC with all the essential attributes is used in the dispute. For this purpose: a digital signature assisted by the TTP-U is encouraged for various advantages. Based on the role of non-repudiation. The TTP-U is classified as a) offline TTP, b) an online TTP, c) an inline TTP, whereas, in the more advanced design, the use of TTP-U will be eliminated if an alternate scheme exists for the dispute resolution.

A suitable design of normal transactions is exhibited in Fig. 1 to highlight the non-repudiation system mechanism. It can be considered as a generalized form of technique towards non-repudiation. In such a scheme, the user feeds their credentials in the form of user identity and password, followed by the generation of the first authentication factor in the user system side. An authenticator node further assesses this information, further carrying out second-factor authentication. This process takes place within the service provider (or another node). However, prior to generating the secondary token, the authenticator must access the user private key from the hardware security module. The extracted information by the authenticator node then successfully generates a second-factor token and thereby completes the dual authentication system. The transactional information generated by the hardware security model is then forwarded to authentication to digitally sign it. However, the biggest challenge in this mechanism is the presence of common attackers, e.g., key loggers, trojans, man-in-middle attacks, man-in-the-browser, internal attacks, etc. Hence, user applications could be extremely vulnerable during the manipulation of information storage. Hence, ensuring non-repudiation becomes quite a challenging aspect of network security. Apart from this, existing studies are found not much-adopted scrutiny towards non-repudiation of origin or emission [12]. Basically, non-repudiation of origin refers to the connection between a communication channel between the sender of the message and the receiver of the message that can offer legitimate evidence of the source of a message. On the other hand, a disclaimer of emission refers to the relationship between the content of the message and its source sender as proof of the sender. The essential design requirement of an efficient NR-Protocol includes: a) fairness, b) efficiency, c) timeliness, d) policy, e) verifiability of TTP-U, and f) transparency, where the verifiability and transparency introduce trade-off which is a challenging task while design N.R. protocols.

B. Multiparty Non-Repudiation

There are many transactions where more than two parties have been involved in the case of multi-party. Therefore, the multi-party non-repudiation problem is different from the two-party N.R. problem. If 'N' parties such that, N>2, exchanges messages and subsequent evidence of transactions are collected, which can be used to settle the dispute if any, then it is said to be a general case of multiparty Non-Repudiation (MP-NR). The MP exchange may be either one too many, many to one, or many, maintaining various topologies like star or mesh. The scenario of MP-exchange, M= {M1, M2, M3, M4} cannot adopt an N-Party NR-protocol, where N=2 because the efficiency will not be optimal as the correlation among MP, cannot be maintained for any unique transaction. Therefore, a suitable Multi-party Non-Repudiation Protocol (MP-NRP) for multi-party exchange should be designed with appropriate design goals of fairness, confidentiality, efficiency, timeliness, and policy. Fig. 2 highlights the multi-party computing model's conceptual architecture and the basic security requirements to counter attacks on cloud-assisted and IoT-enabled ubiquitous and smart applications. Also, a fault-tolerance system is an essential part of security to ensure the reliability of both conventional and distributed computing models.

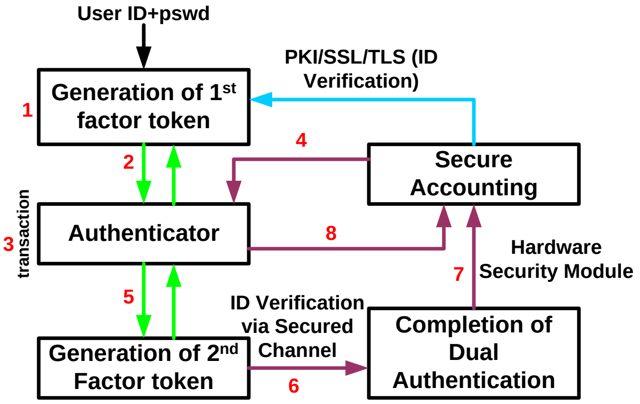
User ID+pswd
PKI/SSL/TLS (ID Verification)
1
Generation of 1st factor token
2
4
Secure Accounting
3
transaction
Authenticator
8
Hardware Security Module
7
5
ID Verification via Secured Channel
Generation of 2nd Factor token
6
Completion of Dual Authentication

Fig. 1. Generalized Design Process of Transaction.

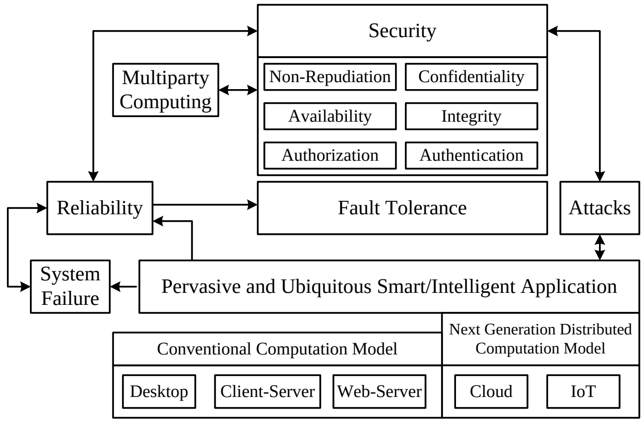

Fig. 2. Conceptual Computing Model and Security Requirements.

III. Methodology for Data Collection

The scope of the digital security system is very vast; therefore, in the initial stage of the study, the keyword-based on the 'non-repudiation' provides the following statistics. Although there are many other reputed journals like Springer, Elsevier, Inder- science Wiley, IGI, NCBI, etc. However, IEEE digital library offers an easy-to-use digital library to find the appropriate problem statement after understanding the current research trend and gap analysis. The data from the IEEE is considered during this initial phase of the study. The timeline of these publications was found from 1994 till 2022, which shows that the research in the field of non-repudiation is always active as throughout the time, The various new networks and communication-based applications evolves on the digital platform and that make the system dynamics. Therefore, the legacy solutions to non-repudiation do not fit the newly developed system. Therefore, to understand the current trend, the literature of only the last five years' publications of the conference and journals is segregated. The statistics found for the same are as tabulated in Table I.

Generally, the IEEE journals and transactions papers are of exceptionally high reputation, so the '34' reports are initially analyzed, whose time stamping from 2015 till 2022 as seen in Table II. The next section discusses about the existing studies toward non-repudiation followed by multiparty-based non-repudiation techniques.

TABLE I. Statistics of Publication on Non-repudiation

Type	Number
Conference	785
Journal	87
Magazine	9
Early Access	6

TABLE II. Statistics of Selected Publications

Type	Number
Conference	305
Journal	69

IV. Study Towards Non-repudiation

This section discusses the existing approaches carried out in different areas of implementation towards addressing the non-repudiation problem.

A. *Securing Adhoc Networks Scheme*

The ad-hoc technology, Smart On-Board Units (s-OBU) and Smart Road Side Units (s-RSU) make the realization of the Vehicular ad-hoc Network (VANETs), where the infotainment system that provides data communication of all types, either sensor data, images, or the video takes place seamlessly and provides passengers conform and safety application and fulfill the vision of intelligent transport system. There has been a tremendous effort towards building such an ecosystem of the network, but there are many security challenges, and the existing security mechanism is ineffective. The work carried out by Pan et al. [13] has presented a secure data sharing methodology using edge computing. The security of the data is offered using the encryption approach of ciphertext policy attributes. Further study towards ensuring non-repudiation was carried out by Baee et al. [14], where an authentication framework is presented. The author has also discussed the significance of using key management and encryption-based approach for securing communication systems in vehicular networks. The existing system mainly emphasizes an authentication scheme towards ensuring a non-repudiation system. Work in such direction was reported by Alfadhi et al. [15], where a hash-based function is developed to perform authentication that further reduces redundancy of authentication. Further, the study implementation of Abbasi et al. [16] has presented a clustering approach using trust and reputation to offer better non-repudiation in vehicular networks. Another study carried out by Fang et al. [17] has emphasized using blockchain and digital signature. The repudiation attacks occur in the VANET, where the attacker denies the participation of sending and receiving the messages. Due to this, the trusted authority gets confused about the audit. The authors, Azees et al. [18], have surveyed the research work towards the non-repudiation in the VANET, and the key finding of those works is tabulated in Table III. In the mechanism suggested by Jie Li et al. [19], whenever the malicious vehicle transmits a fraudulent message and denies the transmission of that message, the trusted authority opens the signature in the message to reveal the actual identity of the vehicle. Though this method provides a cost-effective solution, certificate management is quite challenging in this method. To overcome the problem of the overhead of the certificate management in the PKI-based cryptosystem, the authors Choi and Jung [20] proposes an ID-based cryptosystem to provide non-repudiation. In this scheme, a timestamp is encoded with the date and the time of the message encoded and defines the message validity time. The biggest challenges in all these approaches are that they must be supported by the mobility-prone network, which is not offered with evidence Table III highlights the advantages and issues associated with all these approaches. This scheme cannot ensure strong non-repudiation because of the critical escrow problem of the I.D.-based systems. The authors Biswas and Misic [21] designed a scheme for the non-repudiation of the privacy-preserving authentication in VANET to prevent the repudiation attack. In their system, a signature is created for each message, and to sign the message, each sender needs to have a unique secret key and a session parameter. Once the sender signs the message and sends it, then they cannot deny the signature for the broadcast message. Table III summarizes the important implementation work towards securing an ad-hoc network scheme to ensure non-repudiation.

TABLE III. KEY FINDINGS FOR NON-REPUDIATION IN VANET

Ref	Problem	Technologies Used	Pros	Cons
Pan [13]	Delay due to Data sharing	Edge computing	Offers confidentiality	Induce network overhead
Baee et al. [14]	Secure communicatio n	Authentication	Generalized architecture	Not benchmarked
Alfadh i et al. [15]	Privacy protection	Hash-based authentication	Reduced computational cost	Not resistive for physical attacks
Abassi et al. [16]	Transmission reliability	Clustering algorithm	Robust and validated scheme	Not applicable for dynamic attackers
Li et al. [19]	ACPN	PKC, Digital Signature	Cost-effective	manage certificate
Choi et al. [20]	Certificate overhead	ID-based Cryptos	Time validity	non-repudiation, key escrow problem
Biswas [21]	N.R. privacy	Message signature	Repudiation attack	Overhead of signature

1) Identified research gap: The VANET is a dynamic network where the system works in a decentralized manner; therefore, a method is required to mitigate the effect of the repudiation attack that should have significantly less computational overhead and yet be very effective supports the distributed computing paradigms. Therefore, a multi-party computation-based non-repudiation protocol is advised.

B. Certificateless Scheme

This form of scheme targets to resist the critical escrow issue in network security. A dedicated module called certificate authority generates secret keys that possess complete trust factors within it [22]. For adequate security, this mechanism uses a key generation center and user where the splitting of the secret key is carried out. The work carried out by Zhang et al. [23], Li et al. [24], Won et al. [25], and Islam et al. [26] has used certificates scheme with a different focus on implementation, viz. securing 5G communication, access control on a wearable device, smart city, and enhancing encryption, respectively.

1) Identified research gap: Although this scheme is claimed to offer security concerning non-repudiation, it fails to fully optimize the information associated with the identity of the nodes to generate the public key. It also introduces dependency towards the publishing process for the user's public key. Another significant issue in this approach is that this scheme offers too many usages of encrypting information; however, the decryption process depends on only one private key. Hence, such a mechanism cannot provide resiliency against forged third-party users.

C. Conventional Cryptographic Measures

The conventional cryptographic measures make use of key-based approaches as well as encryption approaches. Existing systems offer many schemes that only emphasize these approaches to provide non-repudiation. The work carried out by Shim et al. [27], and Lin et al. [28] have used key-based methods while the work carried out by Li et al. [29], Amerimehr et al. [30], Zia et al. [31], Randriamasy et al. [32], and Tseng et al. [33] have used encryption-based method. All these approaches are meant for different research problems associated with strengthening the security scope of the application.

1) Identified research gap: The significant issue in adopting conventional cryptographic measures is that none of the mentioned studies have considered device-related complexity issues. Implementing key management will also demand storage, processing, and updating of the key, which consumes extra buffer in resource-constrained devices that have not been addressed. Further usage of encryption has not been testified for its capability towards resisting different forms of threats.

D. Privacy and Authentication Measures

Privacy and authentication are highly connected. The communicating nodes should be secured to prevent their private information from being vulnerable. One way to offer better security is to provide privacy preservation approaches and authentication techniques. Approaches towards privacy preservation are seen in the work of [34]-[35], while some authentication approaches are seen in the creation of [36]-[37]. These studies have strengthened non-repudiation; however, it was not the only focus.

1) Identified research gap: These approaches focus more on privacy and authentication; however, no claim was found to offer faster response time. Response time is required for ensuring a lightweight encryption approach. Existing approaches are also proven to be scalable for the extensive communication environment. Apart from this, there are also various other miscellaneous approaches, e.g., blockchain [38], [39], [40], and various other analytical approaches [41]-[42]. All these approaches are focused on the split form of problems in a wireless network as well as they are also found to be quite specific towards solving methodologies. They cannot leverage any form of flexibility and scalability when different network conditions are applied. Hence, there is a broader scope of improvement towards these approaches for strengthening the non-repudiation issue. The next section discusses existing methods to multi-party non-repudiation schemes.

V. Study Towards Multi-party Schemes

The multi-party based non-repudiation process is widely used in the context of the applications like online auction/bidding systems, business to business/business to consumer, e-commerce, multicast-based collaborative applications, secure cloud storage, secure group encrypted e-mail, securing tender information from the bidders, contract signed by multiple organizations, securing keys in the authentication system, e-mail system, certified notification, etc. The popular methods and technologies used for these systems include PKI, Hash, group encryption, TTP-free methods, source authentication, and schemes to mitigate the effect of non-repudiation attacks. Blockchain has been found to design a multi-party non-repudiation scheme in recent times. The section below describes the researcher's various approaches in this context.

Electronics bidding is one process that mandatory require efficient security. The method proposed by Curtis et al. [43] provides a scalable system designed with essential cryptographic functions. The method isolated the bidder's identities among two core units of the scheme with the assumption that they could not collude. The registration process uses PKI with hash and is controlled by the registration authority to guarantee non-repudiation between all the participants as an auctioneer and the actual wined of the bid. This approach of a registration authority is helpful in many other applications as a framework for the design of effective, secure multi-party transactions.

The basic design of the cryptosystem always considers the hardness of the Discrete Logarithm Problem (DLP), and a typical DLP is described as if a group 'G' such that 'g' is the generator of the group and 'h' is the element of 'G', then the discrete logarithm to the base 'g' of 'h' in a group 'G'. This problem becomes more challenging if the Pohlig -Hellman algorithm cannot solve the DLP very quickly, and it can happen only if DL-cryptosystem Zp, where p is a prime number such that p-1=2q {significant prime factor}. The authors Yanping and Liaojun [44] propose an MPNR protocol based on DLP and group encryption. In any of the online platforms of the enterprises, either in the form of business to business or business to consumer, there are the different digital processes involved, including 1) item request, 2) documents transaction for agreements, 3) payment, 4) different contracts and 5) acknowledgment in a single batch or a group.

In the designed scheme, the stakeholder can direct another message to multiple distinguished recipients to remove exchanges of the same message. It also utilizes the offline Trusted Third Party (TTP), which alleviates the cons of the use of the online TTP and provides better efficiency. The Alternative Time Temporal Logic (ATL) is a variant of the Computational Tree Logic (CTL), used in many contexts where multiple parties are involved for controllability. One of the MPNR methods based on ATL is proposed by Wang et al. [45] to make it useful in e-commerce by adding time limits to each stakeholder so that it acquires a time-independent and fair transaction. Another approach applicable for commencing is proposed by the authors, Wang and Wang [46], use group encryption to design MPNR without using a TTP and validate the model using a popular cryptographic model validation method, namely SVO logic. In the era of collaboration, a scalable architecture based on multicast communication provides a platform to build business models involving multi-party as a stakeholder.

To secure such frameworks, a Secure Multicast Communication (SMC) is desired where the packet overhead and computational efficiency is to be optimal. The most significant problem for SMC is designing an authentication model for the sources. The authors Eltaief and Youssef [47] propose a model for SMC in the context where the communication channel is compromised by the attackers who work on the integrity of the data. The model exploits a multi-layer connected chain structure to build secure multicast authentication. It adjusts the effect of the packet loss but ensures non-repudiation of the origin of the source.

In the era of globalization, where the global network concept is emerging, the role of cloud systems is most important. There is always a hiccup to migrate their data to the cloud system unless they are not assured of the strength and guarantee of security. The authors, Feng et al. [48], highlight their work related to the different issues of security, including 1) fairness, 2) roll-back attack, and 3) repudiation. The method suggested by them for MPNR protocol ensures proper storage in the cloud system with non-repudiation and handles the roll-back attacks. Another model told by Feng et al. [49] focuses on the data integrity aspect during cloud storage by identifying vulnerabilities in popular cloud storage providers. Based on identifying the repudiation problem, a novel MPNR scheme fixes the issue and justifies mitigation of the effect of various network attacks [33].

To design a robust system of authentication schemes, the security of keys plays a vital role. Mandal and Mohanty [50] propose a TTP method to generate the keys and distribute them to respective groups. The security analysis reveals its strength against various attacks, including 1) the non-repudiation attack, 2) replay attack, 3) chosen cipher attack, and 4) man-in-the-middle attack. The protocol can use for various applications like a) group encrypted e-mail multicast in the defense sector, b) securing tender information from the bidders, c) contract signed by multiple organizations, etc.

The traditional benchmarked approaches of the multi-party fair exchange protocol demand more communication cost if applied to other networks' topologies different than mesh topology. The authors Shiraishi et al. [51] found that if the mesh topology strategy is used for the line topology, its performance degrades. To overcome this issue, they propose an N-party certified e-mail protocol for line topology with fairness, non-repudiation, trusted third party invisibility, and timeliness in less communication cost. An application like certified notification requires a fair exchange with strong proof and non-repudiation of the message's origin and exchange. The authors Payeras-Capellà et al. [52] introduce a Multiparty Fair Certified Notification (MFCN)-scheme based on blockchain. The system allows to sending simultaneously certified notifications to the group of receivers. It validates the strategy to achieve better security properties, including a) confidentiality, b) fairness, and c) timeliness with a stateless

TTP. Table IV highlights research towards multi-party non-repudiation schemes along with the associated research gap being explored.

TABLE IV. RESEARCH TOWARDS MULTI-PARTY NON-REPUDIATION SCHEME

Citation	Application	Problem	Approaches
Curtis et al. [43]	Securing Bidding system	Registration authority	PKI, Hash
Yanping et al. [44]	B2C and B2B	DLP Model	Group encryption, offline TTP
Wang et al. [45]	e-commerce	ATL	Adding time limit
Wang et al. [46]	e-commerce	SVOL	Group encryption
Wang et al. [47]	Multicast communication	chain structure	Source authentication
Feng et al. [49]	Cloud Storage	vulnerabilities for repudiation	Overcome non-repudiation
Mandal et al. [50]	Authentication system	Key security	Resistive to non-repudiation attack
Shiraishi et al. [51]	e-mail system	Line topology	Less communication cost without TTP
Payeras et al. [52]	Certified notification	stateless TTP	Blockchain

1) Identified research gap: There are various schemes towards multi-party non-repudiation schemes, where authentication is the prime focus. However, most of the deployed security techniques towards this don't consider the dynamic attribute of the user/node present in the network. This form of implementation can successfully stop one specific form of attack; however, they fail to identify when the attacker changes their attack strategy. The validation of different parties involved in this process is checked only once during the entire simulation. In contrast, there is a fair possibility of inclusion of new kinds of intrusion, or one of the nodes could possibly go rogue. Hence, the existing multi-party non-repudiation system is highly symptomatic and operational over a smaller network and with apriori information of types of attackers.

The next section discusses the open-end research problems identified from the existing review work.

VI. OPEN RESEARCH ISSUES

After reviewing the existing approaches, it has been seen that it has addressed various security problems associated with the different network variants. Therefore, each technique has its scope of implementation while also related to multiple pitfalls. Although all the approaches are liked with the usage of encryption measures, key-based procedures, Certificateless schemes, privacy and authentication schemes, etc., all of these techniques have been specifically meant to address a particular set of problems. The multiparty-based approach is one of the best options; however, they still suffer from various issues concerning non-repudiation as well as it also requires inclusion. The significant problems that are found to be yet an open-end are as follows.

A. Network-Specific Solution

It has been noticed that existing schemes for non-repudiation have been mainly carried out toward specific groups of networks viz. convention network, 5G, Big Data, IoT, vehicular network, cloud environment, wireless sensor network, etc. It should be noted that each network form has its way of incorporating security, which is unique from each other. However, some security protocols may be quite common in this form. A closer look into Table III highlights that maximum work has been attempted to date in the vehicular network. In contrast, many works are carried out on sensory application and IoT (5G). It is well-known that 5G, IoT, and cloud are future technologies and require more security strength to offer better non-repudiation. However, multi-party is not equally focused on these networks.

B. Authentication Flexibility on Different Networks

Existing approaches have used authentication within a significantly narrower scope of its applicability. It should be noted that authentication approaches for different network forms have other dependencies. There is less work to address authentication among massive devices present in IoT. The majority of the applications currently in upcoming times will use IoT, and hence there is a drastic need to incorporate robust authentication measures.

C. Strengthening Multiparty-based Approach

Multiparty-based authentication approach is one of the most robust techniques to offer security. However, existing studies have not provided any form of evidence toward assuring the resiliency of the trusted third party involved in this process. There is a need to incorporate a secure encryption mechanism that can offer robust privacy and non-repudiation while using a multi-party-based approach. A lightweight encryption policy with a faster key management mechanism is the most effective mechanism that can be opted for strengthening non-repudiation issues in dynamic networks.

D. Mechanism of Validation

The majority of the existing approaches towards multiparty-based schemes have not witnessed any standard validation approach. There is a possibility of including any number of multi-party-based authentication systems; hence, there is a need for a cost-effective solution towards a validation approach using unique performance parameters.

E. Computational Complexity

The inclusion of a multiparty-based solution could also offer a potential computational complexity when it comes to validating the stream of data or service requests. In such a case, including an encryption mechanism will further elevate the problem over a wireless network. Apart from this, encryption is a highly iterative operation. At the same time, it is required to offer a good balance between communication and computation, which is not found in existing approaches.

VII. CONCLUSION

This paper has presented a review of the non-repudiation system where the investigation is mainly to check the effectiveness score in involving a multi-party system. After reviewing all the related research approaches, there are various conclusive remarks. It has been identified that the existing studies towards security have a splitting form of implementation towards non-repudiation. Some models a direct non-repudiation system, while others implement a different technique to ascertain non-repudiation. The frequencies of former approaches are comparatively less in contrast to later forms of policies. Also, very few works have implemented the multi-party mechanism to perform validation or security authentication. Besides, multi-party mechanisms developed in the existing system are too specific to network type. Unfortunately, they offer a reduced scope of practical implementation. It should be noted that techniques, e.g., cloud and IoT, integrate multiple forms of other networking systems. A closer look into Table III shows that studies were not focused on cloud and IoT systems, which is required in the existing approach.

More studies on authentication mechanisms have been carried out, but they are not entirely using multi-party computation systems. On the other hand, multi-party computation/validation studies have lacked novel authentication mechanisms. On the other hand, the existing studies where both multi-party authentication systems have been addressed do not deploy a computationally cost-effective technique. There is no report of practical scenario if it runs over resource-constrained devices.

Therefore, our future work will develop a comprehensive model of a multi-party computational system that can offer a superior form of non-repudiation in a dynamic network. The study will consider the use case of IoT systems hosted over a cloud environment. It will be meant towards bridging the gap in current research work.

References

[1] B. Nayak, M. Mangla, S. N. Mohanty, S. Satpathy, Integration of Cloud Computing with Internet of Things Foundations, Analytics and Applications, Wiley, ISBN: 9781119769309, 1119769302, 2021.

[2] A. Nagaraj, Introduction to Sensors in IoT and Cloud Computing Applications, Bentham Science Publishers, ISBN: 9789811479335, 981147933X, 2021.

[3] H. Pham, Reliability and Statistical Computing Modeling, Methods and Applications, Springer International Publishing, ISBN: 9783030434120, 3030434125, 2020.

[4] D. C. Wilson, Cybersecurity, MIT Press, ISBN: 9780262542548, 0262542544, 2021.

[5] B. Gordijn, M. Christen, M. Loi, The Ethics of Cybersecurity, Springer International Publishing, ISBN: 9783030290535, 3030290530, 2020.

[6] D. Evans, V. Kolesnikov, M. Rosulek, A Pragmatic Introduction to Secure Multi-Party Computation, Now Publishers, ISBN: 9781680835083, 1680835084, 2019.

[7] M.E. Whitman, H.J. Mattord, Principles of Information Security, Cengage Learning, ISBN: 9780357506561, 0357506561, 2021.

[8] D. Chatterjee, Cybersecurity Readiness-A Holistic and High-Performance Approach, SAGE Publications, ISBN: 9781071837351, 1071837354, 2021.

[9] L. Bock, Modern Cryptography for Cybersecurity Professionals-Learn how You Can Leverage Encryption to Better Secure Your Organization's Data, Packt Publishing, ISBN: 9781838647797, 1838647791, 2021.

[10] M. Chapple, Access Control and Identity Management, Jones & Bartlett Learning, ISBN: 9781284198355, 1284198359, 2020.

[11] Onieva, Jose A., Jianying Zhou, and Javier Lopez. "Multi-party non-repudiation: A survey." ACM Computing Surveys (CSUR) 41, no. 1 (2009): 1-43.

[12] I. Symeonidis, D. Rotaru, M. A. Mustafa, B. Mennink, B. Preneel and P. Papadimitratos, "HERMES: Scalable, Secure, and Privacy-Enhancing Vehicular Sharing-Access System," in IEEE Internet of Things Journal, vol. 9, no. 1, pp. 129-151, 1 Jan.1, 2022, doi: 10.1109/JIOT.2021.3094930.

[13] J. Pan, J. Cui, L. Wei, Y. Xu & H. Zhong, "Secure data sharing scheme for VANETs based on edge computing", Springer-EURASIP Journal on Wireless Communications and Networking volume 2019.

[14] M.A.R. Baee, L. Simpson, X. Boyen, E. Foo, & J. Pieprzyk, "Authentication strategies in vehicular communications: a taxonomy and framework", Springer-EURASIP Journal on Wireless Communications and Networking, 2021.

[15] S.A. Alfadhli, S. Lu, A. Fatani, H. Al-Fedhly, & M. Ince, "SD2PA: a fully safe driving and privacy-preserving authentication scheme for VANETs",Springer-Human-centric Computing and Information Sciences, volume 10, Article number: 38, 2020.

[16] R. Abassi, A. B. C. Douss & D. Sauveron, "TSME: a trust-based security scheme for message exchange in vehicular Ad hoc networks"Springer-Human-centric Computing and Information Sciences volume 10, Article number: 43, 2020.

[17] W. Fang, W. Chen, W. Zhang, J. Pei, W. Gao & G. Wang, "Digital signature scheme for information non-repudiation in blockchain: a state of the art review", Springer-EURASIP Journal on Wireless Communications and Networking volume 2020, Article number: 56, 2020.

[18] M. Azees, P. Vijayakumar and L. Jegatha Deborah, "Comprehensive survey on security services in vehicular ad-hoc networks," in *IET Intelligent Transport Systems*, vol. 10, no. 6, pp. 379-388, 8 2016. doi: 10.1049/iet-its.2015.0072.

[19] Jie Li, Huang Lu, et al.: 'ACPN: A Novel Authentication Framework with Conditional Privacy-Preservation and Non-Repudiation for VANETs', IEEE Transactions on Parallel and Distributed Systems, 2014, 26, (4), pp- 938 – 948.

[20] Choi, J., Jung, S., 'A security framework with strong non-repudiation and privacy in VANETs'. In Proceedings of the 6th IEEE Conference on Consumer Communications and Networking Conference table Las Vegas, NV, USA, 2009, pp: 835-839.

[21] Biswas, S., Misic, J., 'A cross-layer approach to privacy-preserving authentication in WAVE-enabled VANETs, IEEE Transactions on Vehicular Technology, 2013, 62, (5), pp. 2182–2192.

[22] Rezaeibagha, Fatemeh, Yi Mu, Xinyi Huang, Wenjie Yang, and Ke Huang. "Fully secure lightweight certificateless signature scheme for IIoT." IEEE Access 7 (2019): 144433-144443.

[23] Y. Zhang, F. Ren, A. Wu, T. Zhang, J. Cao and D. Zheng, "Certificateless Multi-Party Authenticated Encryption for NB-IoT Terminals in 5G Networks," in *IEEE Access*, vol. 7, pp. 114721-114730, 2019. doi: 10.1109/ACCESS.2019.2936123.

[24] F. Li and J. Hong, "Efficient Certificateless Access Control for Wireless Body Area Networks," in *IEEE Sensors Journal*, vol. 16, no. 13, pp. 5389-5396, July1, 2016. doi: 10.1109/JSEN.2016.2554625.

[25] J. Won, S. Seo and E. Bertino, "Certificateless Cryptographic Protocols for Efficient Drone-Based Smart City Applications," in *IEEE Access*, vol. 5, pp. 3721-3749, 2017. doi: 10.1109/ACCESS.2017.2684128.

[26] S. Hafizul Islam and F. Li, "Leakage-Free and Provably Secure Certificateless Signcryption Scheme Using Bilinear Pairings," in *The Computer Journal*, vol. 58, no. 10, pp. 2636-2648, Oct. 2015. doi: 10.1093/comjnl/bxv002.

[27] K. Shim, "A Survey of Public-Key Cryptographic Primitives in Wireless Sensor Networks," in *IEEE Communications Surveys & Tutorials*, vol. 18, no. 1, pp. 577-601, Firstquarter 2016. doi: 10.1109/COMST.2015.2459691.

[28] J. Lin, W. Zhu, Q. Wang, N. Zhang, J. Jing and N. Gao, "RIKE+ : using revocable identities to support key escrow in public key infrastructures with flexibility," in *IET Information Security*, vol. 9, no. 2, pp. 136-147, 3 2015. doi: 10.1049/iet-ifs.2013.0552.

[29] F. Li, D. Zhong and T. Takagi, "Efficient Deniably Authenticated Encryption and Its Application to E-Mail," in *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 11, pp. 2477-2486, Nov. 2016.

[30] A. Amerimehr and M. H. Dehkordi, "Quantum Symmetric Cryptosystem Based on Algebraic Codes," in *IEEE Communications Letters*, vol. 22, no. 9, pp. 1746-1749, Sept. 2018. doi: 10.1109/LCOMM.2018.2844245.

[31] M. Zia and R. Ali, "Cryptanalysis and improvement of blind signcryption scheme based on elliptic curve," in *Electronics Letters*, vol. 55, no. 8, pp. 457-459, 18 4 2019. doi: 10.1049/el.2019.0032.

[32] M. Randriamasy, A. Cabani, H. Chafouk and G. Fremont, "Formally Validated of Novel Tolling Service With the ITS-G5," in *IEEE Access*, vol. 7, pp. 41133-41144, 2019. doi: 10.1109/ACCESS.2019.2906046.

[33] Y. Tseng, T. Tsai and S. Huang, "Leakage-Free ID-Based Signature," in *The Computer Journal*, vol. 58, no. 4, pp. 750-757, April 2015. doi: 10.1093/comjnl/bxt116.

[34] C. Hu and Y. Huo, "Efficient privacy-preserving dot-product computation for mobile big data," in *IET Communications*, vol. 11, no. 5, pp. 704-712, 30 3 2017.doi: 10.1049/iet-com.2016.0782.

[35] C. Sun, J. Liu, X. Xu and J. Ma, "A Privacy-Preserving Mutual Authentication Resisting DoS Attacks in VANETs," in *IEEE Access*, vol. 5, pp. 24012-24022, 2017. doi: 10.1109/ACCESS.2017.2768499.

[36] M. A. Sahi *et al*., "Privacy Preservation in e-Healthcare Environments: State of the Art and Future Directions," in *IEEE Access*, vol. 6, pp. 464-478, 2018. doi: 10.1109/ACCESS.2017.2767561.

[37] F. Wang, Y. Xu, H. Zhang, Y. Zhang and L. Zhu, "2FLIP: A Two-Factor Lightweight Privacy-Preserving Authentication Scheme for VANET," in *IEEE Transactions on Vehicular Technology*, vol. 65, no. 2, pp. 896-911, Feb. 2016. doi: 10.1109/TVT.2015.2402166.

[38] K. Shim, "Security Analysis of Various Authentication Schemes Based on Three Types of Digital Signature Schemes," in *IEEE Access*, vol. 6, pp. 68804-68812, 2018. doi: 10.1109/ACCESS.2018.2879961.

[39] W. Huang, Y. Liao, S. Zhou and H. Chen, "An Efficient Deniable Authenticated Encryption Scheme for Privacy Protection," in *IEEE Access*, vol. 7, pp. 43453-43461, 2019. doi: 10.1109/ACCESS.2019.2907250.

[40] M. A. Alazzawi, H. Lu, A. A. Yassin and K. Chen, "Efficient Conditional Anonymity With Message Integrity and Authentication in a Vehicular Ad-Hoc Network," in *IEEE Access*, vol. 7, pp. 71424-71435, 2019. doi: 10.1109/ACCESS.2019.2919973.

[41] C. Sun, J. Liu, Y. Jie, Y. Ma and J. Ma, "Ridra: A Rigorous Decentralized Randomized Authentication in VANETs," in *IEEE Access*, vol. 6, pp. 50358-50371, 2018. doi: 10.1109/ACCESS.2018.2868417.

[42] J. Li, H. Lu and M. Guizani, "ACPN: A Novel Authentication Framework with Conditional Privacy-Preservation and Non-Repudiation for VANETs," in *IEEE Transactions on Parallel and Distributed Systems*, vol. 26, no. 4, pp. 938-948, April 2015. doi: 10.1109/TPDS.2014.2308215.

[43] B. Curtis, J. Pieprzyk and J. Seruga, "An Efficient eAuction Protocol," *The Second International Conference on Availability, Reliability and Security (ARES'07)*, Vienna, 2007, pp. 417-421. doi: 10.1109/ARES.2007.37.

[44] L. Yanping and P. Liaojun, "Multi-party Non-repudiation Protocol with Different Message Exchanged," *2009 Fifth International Conference on Information Assurance and Security*, Xi'an, 2009, pp. 491-494.doi: 10.1109/IAS.2009.329.

[45] X. Wang, "Formal Analysis and Improvement of Multi-Party Non-Repudiation Protocol," *2009 5th International Conference on Wireless Communications, Networking and Mobile Computing*, Beijing, 2009, pp. 1-4.doi: 10.1109/WICOM.2009.5302343.

[46] X. Wang and X. Wang, "Formal Analysis Of Multi-party Non-repudiation Protocols Without TTP," *2010 International Conference on Communications and Intelligence Information Security*, Nanning, 2010, pp. 96-99.doi: 10.1109/ICCIIS.2010.33.

[47] H. Eltaief and H. Youssef, "Efficient sender authentication and signing of multicast streams over lossy channels," *ACS/IEEE International Conference on Computer Systems and Applications - AICCSA 2010*, Hammamet, 2010, pp. 1-7.doi: 10.1109/AICCSA.2010.5586962.

[48] J. Feng, Y. Chen, D. Summerville, W. Ku and Z. Su, "Enhancing cloud storage security against roll-back attacks with a new fair multi-party non-repudiation protocol," *2011 IEEE Consumer Communications and Networking Conference (CCNC)*, Las Vegas, NV, 2011, pp. 521-522. doi:10.1109/CCNC.2011.5766528.

[49] J. Feng, Y. Chen and D. H. Summerville, "A fair multi-party non-repudiation scheme for storage clouds," *2011 International Conference on Collaboration Technologies and Systems (CTS)*, Philadelphia, PA, 2011, pp. 457-465.doi: 10.1109/CTS.2011.5928724.

[50] S. Mandal and S. Mohanty, "Multi-party Key-Exchange with Perfect Forward Secrecy," *2014 International Conference on Information Technology*, Bhubaneswar, 2014, pp. 362-367. doi: 10.1109/ICIT.2014.30.

[51] Y. Shiraishi, M. Mohri, H. Miyazaki and M. Morii, "A Three-Party Optimistic Certified Email Protocol Using Verifiably Encrypted Signature Scheme for Line Topology," *2015 IEEE 2nd International Conference on Cyber Security and Cloud Computing*, New York, NY, 2015, pp. 260-265. doi: 10.1109/CSCloud.2015.64.

[52] M. Payeras-Capellà, M. Mut-Puigserver and M. À. Cabot-Nadal, "Smart Contract for Multiparty Fair Certified Notifications," *2018 Sixth International Symposium on Computing and Networking Workshops (CANDARW)*, Takayama, 2018, pp. 459-465. doi: 10.1109/CANDARW.2018.00089.